HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/81C

16 March 2016

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Operational Incidents Watch

The Hong Kong Monetary Authority published today the enclosed fifth issue of Operational Incidents Watch.

The Operational Incidents Watch is a periodic newsletter to share with the industry the major lessons learnt from selected significant operational incidents that have happened in the banking sector. It aims at facilitating authorized institutions (AIs) and members of the public in Hong Kong to stay alert and to take appropriate measures to prevent similar incidents from happening to them. In this connection, we expect AIs' senior management to ensure that their relevant business lines and operational risk management functions will take into account the Operational Incidents Watch to review and enhance where appropriate the relevant risk management controls, including any applicable customer education efforts.

If there are any questions on this Operational Incidents Watch, please contact Mr Parry Tang at 2878-1524 or Ms Debora Chan at 2878-1593.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)

Encl.

55th Floor, Two International Finance Centre,
8 Finance Street, Central, Hong Kong
Website: www.hkma.gov.hk

香港中環金融街8號國際金融中心2期55樓
網址：www.hkma.gov.hk

Issue No. 5
16 March 2016

Operational Incidents Watch is a periodic newsletter published by the Banking Supervision Department of the Hong Kong Monetary Authority (HKMA). It summarises the major lessons learnt from selected operational incidents[1] that have happened in the banking industry and led to impact on relevant customers or material financial losses of the authorized institutions (AIs) concerned. It aims at facilitating AIs and members of the public in Hong Kong to stay alert and to take appropriate measures to prevent similar incidents from happening to them.

In this newsletter, the modus operandi or the factors and key control loopholes leading to two operational incidents are outlined: (i) ineffective call-back verification on third-party fund transfers; and (ii) mistake in allowing an authorized person to bring in another person when accessing a safe deposit box.

Ineffective call-back verification on third-party fund transfers

A number of fraudulent fund transfer transactions were executed by an AI due to ineffective call-back procedures carried out by its staff.

Modus operandi / factors leading to the incident

The victim customer, who resided in an overseas jurisdiction, maintained a bank account with the AI. A fraudster mailed to the AI a fraudulent written request with a forged signature for changing the contact information of the customer, including her mobile phone number, home phone number and email address. Upon receiving the request, call-back verification was conducted by a staff member of the AI using the customer's original phone number recorded in the AI's system and some static customer information. As the person who received the AI's phone call might have already got hold of the personal information of the victim, she managed to answer

[1] Because of sensitivity, the incidents mentioned in this newsletter may be prepared on the basis of synthesis of multiple incidents and certain details of the incidents may deliberately be omitted.

the call-back verification questions. Accordingly, the staff member proceeded to update the customer's contact information in the AI's system.

A few days later, the AI received several mail-in written instructions to transfer funds out of the customer's account. The fraudster also called and requested the AI not to mail the account statements but send the statements in electronic copies to the new email address. To verify the genuineness of these instructions, staff members of the AI contacted the customer using the new mobile phone number and asked verification questions on the static information of the customer. While the fraudster failed to provide correct answers to some of the verification questions, the staff members still effected the fund transfer transactions. The unauthorized transactions were subsequently detected by the AI only when one of them could not be processed due to errors in the beneficiary information. Although the customer was reluctant to report the case to the local law enforcement agency, the AI reported the matter to the Hong Kong Police Force and carried out an in-depth investigation and look back reviews.

Control loopholes and lessons learnt

i. Subsequent to the incident, the AI has enforced perfect match requirement on relevant call-back verification procedures (including those involving high risk situation) and has reviewed the related escalation procedures. Dynamic questions may also be asked during the verification under potentially high-risk circumstances.

ii. Additional authentication technologies will be rolled out by the AI to cover customers residing outside Hong Kong. Alert messages in the form of SMS notifications will also be sent to customers for high-risk transactions such as outflow of funds with a significant amount.

Mistake in allowing an authorized person to bring in another person when accessing a safe deposit box

The incident involved a branch staff member of an AI who mistakenly allowed an authorized person to enter the safe deposit box area together with her relative who was not an authorized person of the relevant safe deposit box.

Modus operandi / factors leading to the incident

The safe deposit box holder assigned her mother as an authorized person of the safe deposit box so that access to the box would be granted with either one of the two specimen signatures.

On one occasion, the authorized person (i.e. the mother) visited the branch with a man, who was her relative, to access the safe deposit box. At the request of the branch staff member, both of them signed on the form but the staff member mistakenly presumed that they were the holder and the authorized person of the safe deposit box. The staff member verified the signature of the authorized person only but not the one from her relative, which was in breach of the AI's policy, and then allowed both persons to enter the safe deposit box area.

The mistake was uncovered during a subsequent check of the signatures on the form and then the branch informed the safe deposit box holder of this incident.

Control loopholes and lessons learnt

i. The importance of exercising sufficient care in verifying the signature(s) of the holder(s) and/or authorized person(s) of a safe deposit box should be emphasized to relevant branch staff members, given that such incidents can pose significant reputational risk to the AI.

ii. At the time of processing the above request for accessing the safe deposit box, the concerned branch staff member, who was relatively new to her position, was also handling a transaction of another customer over the counter. It is important for the branch manager to ensure that all relevant staff members are familiar with the relevant procedures for safe deposit box operations, and remind them to always adhere to the procedures, even though when they are busy in handling other counter transactions or serving other customers.